KENT PETRY (Admitted Pro Hac Vice)
kent@petrylaw.net
LAW OFFICES OF KENT PETRY
1135 Mearns Road, #3387
Warminster, PA 18974
Telephone: 215-322-1084
Facsimile: 215-798-8054

AMY K. SAECHAO (Bar No. 336693)
amy@nextlevellegal.com
NEXT LEVEL LEGAL
6080 Center Drive, Suite 600
Los Angeles, CA 90045
Telephone: 310-426-8823

Attorneys for Plaintiff, Jesus Marcos

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA – EASTERN DIVISION

JESUS MARCOS,

Plaintiff,

v.

T-MOBILE USA, INC., and DOES 1-10,

Defendant(s).

Case No.:

COMPLAINT FOR:

(1) VIOLATIONS OF THE CALIFORNIA ARBITRATION ACT; (2) VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW; (3) VIOLATIONS OF THE FEDERAL COMMUNICATIONS ACT; (4) NEGLIGENCE; (5) NEGLIGENT HIRING, RETENTION TRAINING AND SUPERVISION; (6) GROSS NEGLIGENCE; (7) VIOLATIONS OF THE STORED COMMUNICATIONS ACT; (8) VIOLATIONS OF THE COMPUTER FRAUD AND ABUSE ACT; (9) CONVERSION; (10) CIVIL CONSPIRACY; (11) CIVIL AIDING AND ABETTING; (12) BREACHES OF IMPLEMENTING REGULATIONS OF THE FEDERAL COMMUNICATIONS ACT, 47 C.F.R §64.2001 ET SEQ.; (13) VIOLATIONS OF THE

CALIFORNIA CONSTITUTIONAL RIGHT TO PRIVACY; (14) VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT; (15) BREACH OF CONTRACT; (16) BREACH OF FIDUCIARY DUTY; (17) VIOLATIONS OF THE FAIR CREDIT REPORTING ACT; (18) DECLARATORY JUDGMENT

DEMAND FOR JURY TRIAL

Plaintiff Jesus Marcos, by and through The Law Offices of Kent Petry and undersigned counsel, complains and alleges as follows against T-Mobile USA, Inc ("T-Mobile"):

I. JURISDICTION AND VENUE

1. This Court has original jurisdiction over this matter pursuant to 28 U.S.C. § 1331 because this case arises under federal question jurisdiction under the Federal Communications Act ("FCA"), Stored Communications Act ("SCA"), and the Computer Fraud and Abuse Act ("CFAA").

2. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because the claims are derived from a common nucleus of operative facts.

3. This Court further has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332 as the amount in controversy exceeds $75,000.00, exclusive of interests and costs, and is between citizens of different states where Plaintiff is an individual who is a citizen of the State of California, and Defendant T-Mobile USA, Inc. is a

corporation founded in the Country of Germany, organized in the State of Delaware, with a principal place of business in the State of Washington.

4. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1)-(3) and § 1391(d). Defendant T-Mobile USA, Inc. is subject to personal jurisdiction in this District due to: maintaining substantial contacts within this district; conducting business in this District; and residing in this District. Moreover, a substantial part of the events or omissions giving rise to this claim occurred in this district.

II. PARTIES

5. Plaintiff Jesus Marcos is a male citizen of the United States of America residing in the State of California, Riverside County.

6. Plaintiff, at all relevant times, was a T-Mobile customer who lost hundreds of thousands of dollars in money and cryptocurrency as a result of the actions, inaction and negligence of Defendant.

7. Defendant T-Mobile USA, Inc. is an active corporation founded in the County of Germany, organized in the State of Delaware, with a principal place of business in the State of Washington. Defendant T-Mobile USA, Inc., which is marketed as "T-Mobile," is a wholly-owned subsidiary of T-Mobile US, Inc.

8. Defendant T-Mobile USA, Inc. is engaged in an industry affecting interstate commerce, and at all relevant times has regularly conducted business in the State of California, including Riverside County.

9. Defendant is a "common carrier" governed by the Federal Communications Act, 47 U.S.C. § 151 *et seq*.

10. At all times material hereto, Defendant acted by and through its authorized agents, servants, workers, employees, and/or vendors acting in the course and scope of their employment/agency with Defendant and in furtherance of Defendant's business.

11. Plaintiff is unaware of the names of the additional defendants sued herein under the fictitious names DOES ONE through TEN. Upon information and belief, these may include T-Mobile Third Party Retailers, Third Party Customer Service Centers, or other employees and/or agents of T-Mobile. Defendant T-Mobile USA, Inc. is in exclusive possession of information sufficient to identify those individuals and/or entities who are in some manner responsible for the occurrences herein alleged, proximately caused Plaintiff's damages, and were acting as agent(s) for the others.

III. NATURE OF THE ACTION

12. This action is brought by Plaintiff, a T-Mobile customer who has lost hundreds of thousands of dollars in an incident of an identity theft crime: "SIM swapping" or "SIM hijacking."

13. These crimes are somewhat unique in that they require the negligence, recklessness and/or intentional participation of a consumer's cell phone company, and their employees, agents and vendors.

14. For instance, upon information and belief the unauthorized SIM-swap performed on Plaintiff's account which directly led to the theft of his property was performed utilizing T-Mobile credentials and T-Mobile devices, including an iPad utilized by their stores and employees referred to as a "REMO device."

15. Accordingly, Plaintiff brings causes of action against T-Mobile USA, Inc. and John Does 1-10 as follows: (1) Violations of the California Arbitration Act; (2) Violations of the California Unfair Competition Law; (3) Violations of the Federal Communications Act, 47 U.S.C. § 201 *et seq.*; (4) Negligence; (5) Negligent Hiring, Retention and Supervision; (6) Gross Negligence; (7) Violations of the Stored Communications Act; (8) Violations of the Computer Fraud and Abuse Act; (9) Conversion; (10) Civil Conspiracy; (11) Civil Aiding and Abetting; (12) Violations of the Implementing Regulations of the Federal Communications Act, 47 C.F.R § 64.2001 *et seq.*; (13) Violations of the California Constitutional Right to Privacy; (14) Violations of the California Consumer Privacy Act; and (15) Breach of Contract; (16) Breach of Fiduciary Duty; (17) Violations of the Fair Credit Reporting Act; and (18) Declaratory Judgment.

IV. FACTUAL ALLEGATIONS

a. General

16. T-Mobile markets and sells wireless cellular services through standardized wireless service plans at various retail locations, online and over the telephone.

17. In connection with its provision of wireless services, T-Mobile maintains accounts for its customers, enabling T-Mobile to access information about their customers and the services they have purchased.

18. Numerous large-scale data breaches and thousands of instances of mishandling of customer account information have occurred at T-Mobile. See, e.x., https://firewalltimes.com/t-mobile-data-breaches/ (November 2009: Millions of T-Mobile Customer Records Stolen and Sold; October 2015: Data on 15 Million T-Mobile Subscribers Stolen; October 2017: Website Bug Exposes Customer Data; August 2018: Data on 2 Million T-Mobile Subscribers Stolen; November 2019: Over 1 Million Prepaid T-Mobile Customers Impacted by Data Breach; March 2020: Hacker Accesses T-Mobile Employee Email Data; December 2020: Hackers Access Customer Information on 200,000 Accounts; August 2021: Hackers Steal Data on Nearly 77 Million T-Mobile Customers; January 2023: Hacker Uses API to Access Data on 37 Million Accounts; April 2023: T-Mobile Discloses Second Data Breach of 2023; September 2023: System Error Exposes Data on T-Mobile Customers; September 2023: 89 GB of T-Mobile Employee Data Posted to Hacker Forum.)

19. As a common carrier and one of the nation's largest wireless carriers, Defendant T-Mobile's operations must comply with various federal and state statutes, rules, and regulations, including a duty to protect the confidential personal information of its customers under Section 222 of the FCA, 47 U.S.C. § 222, and to have a written identity theft plan in place under the Red Flags Rule, 16 C.F.R. § 681.1(b) and (d).

20. The FCA obligates Defendant T-Mobile to protect the "confidential proprietary information of [its] customers" and "customer proprietary network information" ("CPI" and "CPNI" respectively). 47 U.S.C. § 222(a), (c).

21. Section 222(a), 47 U.S.C. § 222(a) states that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to …customers…." The "confidential proprietary information" referred to in Section 222(a) is abbreviated herein as "CPI."

22. Section 222(c), 47 U.S.C. § 222(c), states that:

> "[a] telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications services shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (a) the telecommunications services from which such information is derived, or (b) services necessary to, or used in, the provision of such telecommunications service…."

The "customer proprietary network information" referred to in Section 222(c) is abbreviated herein as "CPNI."

23. The Federal Communications Commission ("FCC") has promulgated rules to implement Section 222 of the FCA "to ensure that telecommunications carriers establish **effective** safeguards to protect against unauthorized use or disclosure of CPNI." 1998 CPNI Order, 13 FCC Rcd. At 8195 ¶193 (emphasis added); see also 47 C.F.R. § 64.2001 *et seq.* ("CPNI Rules").

24. The CPNI Rules limit disclosure and use of CPNI without customer approval to certain limited circumstances (such as cooperation with law enforcement), none of which are applicable in the current matter. See 47 C.F.R. § 64.2005.

25. The CPNI Rules also require carriers to implement safeguards to protect customers' CPNI. 47 C.F.R. § 64.2009(b), (d), and (e).

26. These safeguards include: (a) training personnel "as to when they are and are not authorized to use CPNI"; (b) establishing "a supervisory review process regarding carrier compliance with the rules"; and (c) filing annual compliance certificates with the FCC. Id.

27. The CPNI Rules further require carriers to implement measures to prevent the disclosure of CPNI to unauthorized individuals.

28. For example, "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 C.F.R. § 64.2010(a).

29. Moreover, "carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit." Id.

30. In the case of in-store access to CPNI, "[a] telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information." 47 C.F.R. § 64.2010(d).

31. "Valid photo ID" is defined in 47 C.F.R. § 64.2003(r) as "a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired." Id.

32. The FCC has determined that information obtained from customers through a common social engineering plot known as "pretexting" is CPNI. See *In the Matter of Implementation of the Telecommunications Acts of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd. 6927 (2007) ("Pretexting Order").

33. Pretexting is "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records." Id., n. 1.

34. Such "call detail" and "private communications" are CPI and CPNI under the FCA. Id., at 6928 *et seq*.

35. The FCC concluded that "pretexters have been successful at gaining unauthorized access to CPNI" and that "carriers' record on protecting CPNI demonstrate[d] that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI." Id. At 6933. The FCC thus modified its rules to impose additional security for carriers' disclosure of CPNI and to require that law enforcement and customers be notified of security breaches involving CPNI. Id. At 6936-62.

36. In its Pretexting Order, the FCC stated that it "fully expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information." Id. At 6959, ¶64.

37. The FCC further stated that "[w]e decline to immunize carriers from possible sanction for disclosing customers' private information without appropriate authorization." Id. at 6960, ¶66.

38. The FCC stressed the fact that *someone having obtained information fraudulently is strong evidence of the carrier's failure to satisfy the requirements of Section 222*, stating:

> "we hereby put carriers on notice that the Commission henceforth will infer from evidence that a pretexter has obtained unauthorized access to a customer's CPNI that the carrier did not sufficiently protect that customer's CPNI. A carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable in light of the threat posed by pretexting and the sensitivity of the customer information at issue." Id. at 6959, ¶63 (emphasis added).

39. As further alleged herein, Defendant T-Mobile violated Section 222 of the FCA and the CPNI Rules, and further ignored the warnings of the Pretexting Order when on January 23, 2022 T-Mobile performed an unauthorized SIM-swap on Plaintiff's phone, thereby providing control of Plaintiff's phone number and access to

his confidential information to a T-Mobile employee, agent, and/or vendor, or a third-party unknown to Plaintiff, but likely known to T-Mobile.

40. This unauthorized SIM-swap allowed access to Plaintiff's personal information, including CPI and CPNI, without Plaintiff's authorization or permission, and was performed by T-Mobile without validating the identity of the individual requesting that SIM-swap or complying with Defendant's obligations under the FCA, the Red Flags Rule, and other rules, regulations and statutes.

41. Despite T-Mobile's duty to protect the privacy of T-Mobile's customers, T-Mobile has not taken sufficient action to protect their customers from the ongoing onslaught of SIM-swap cases suffered by T-Mobile customers, instead seeking to shift the burden and blame to their customers.

42. For instance, when asked what T-Mobile was doing to address the SIM-swap plague, T-Mobile proffered that they "empower their customers" and seek to dissuade third party bad-actors, rather than take any single action themselves.

43. T-Mobile's policies, procedures and safeguards do nothing to prevent or address internal/dealer fraud, compromised log in information for their own employees or vendors, or the unauthorized access to and use of T-Mobile property (such as REMO devices) to access and make changes to customer accounts. In fact, Defendant T-Mobile has objected to and opposed FCC proposals to require cell phone providers to strengthen customer protections, and continues to perform unauthorized SIM-swaps to their customers' detriment.

b. T-Mobile's Actions and Statements on Privacy and SIM-swaps

44. Defendant T-Mobile regularly holds itself out to the general public as a secure and reliable custodian of customer data, including customers' confidential financial and personal information.

45. Defendant T-Mobile maintains that it uses a variety of "administrative, technical, contractual, and physical safeguards" to protect customers' data against "unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use while it is under our control." https://www.t-mobile.com/privacy-center/our-practices/privacy-policy, as of June 2, 2021.

46. As an example, T-Mobile explicitly states that "when you contact us by phone or visit us in our stores, we have procedures in place to make sure that only the primary account holder or authorized users have access." Id.

47. T-Mobile's sales and marketing materials make similar representations regarding T-Mobile's alleged implementation of various safeguards to protect its customers' private information.

48. As T-Mobile states on their own website, their customers "have a right, and T- Mobile has a duty, to protect the confidentiality of your account information." T-Mobile further has stated that "We take this obligation seriously and do everything possible to ensure that your account information is not shared with others without your consent."

49. T-Mobile further acknowledges its responsibility to protect consumers' "Personal Information" under the FCA, the CPNI Rules, and other statutes and regulations in its Privacy Statement ("Privacy Policy"), Code of Business Conduct ("COBC"), their Terms and Conditions, and T-Mobile's Customer Proprietary Network Information Policy ("CPNI Policy")

50. In T-Mobile's Privacy Policy, COBC, Terms and Conditions, and CPNI Policy, T-Mobile outlines duties and makes binding commitments to Plaintiff, as its customer, that T-Mobile will protect and secure Plaintiff's "Personal Information." The Privacy Policy defines "Personal Information" as "[i]nformation that we directly association with a specific person or entity (for example, name; address; telephone numbers; e-mail address; Social Security Number; call records; wireless device location)." T-Mobile states that, among the information that it collects from and about its customers, are "your name, address, telephone number, e-mail address" along with other CPNI and service-related details such as payment history, security codes, service history, and similar information.

51. When logging into a customer account utilizing T-Mobile software/applications, for example by using a dealer/employee code, this information is presented immediately and directly to the user accessing the account.

52. T-Mobile also collects information relating to the use of its networks, products and services. "Personal Information" thus includes both CPI and CPNI under Section 222 of the FCA and the CPNI Rules.

53. In its Privacy Policy, T-Mobile states: "We use a variety of physical, electronic, and procedural safeguards to protect Personal Information from unauthorized access, use or disclose while it is under our control."

54. There is no evidence that T-Mobile has actually implemented any such safeguards, such as those as might have prevented the SIM-swap on Plaintiff's account utilizing T-Mobile credentials and a T-Mobile device.

55. Similarly, in its CPNI Policy, T-Mobile promises that it "is committed to protecting the privacy and security of our customers' personal information and, as set forth in our Privacy Statement, we strive to be a leader in protecting all such personal information."

56. The T-Mobile CPNI Policy further states:

> Although federal law has long required telecommunications carriers to protect CPNI, in an Order released on April 2, 2007, the Federal Communications Commission ("FCC") issued revised and expanded CPNI rules in response to several high-profile incidents involving the activities of "data brokers" and "pretexters" who attempt to obtain unauthorized access to such information. These rules became effective December 8, 2007 [;] and T-Mobile has implemented policies and safeguard procedures to help ensure compliance. T-Mobile continually reviews its compliance with such rules and annually certifies compliance to the FCC."

57. T-Mobile's COBC also makes binding commitments to Plaintiff, as a T-Mobile customer, that it will protect their Personal Information and that it will adhere

to all its legal obligations. Those legal obligations include, by implication, Section 222 of the FCA, the CPNI Rules, and other legal obligations that govern protection of confidential and private information.

58. For example, T-Mobile's COBC provides:

- "Customers entrust a lot of sensitive information to us – credit card numbers, Social Security numbers, all sorts of things. *** Here's the thing: We protect the confidentiality of our customers' information."
- "When it comes to customer information, we're also careful about access and disclosure. We access this information only when we need to when doing our job – and only to the extent our job duties allow. *** We share customer information only if the customer says we can or we're allowed to by the law, our Terms & Conditions, or Privacy policies."

59. Additionally, T-Mobile took on even more duties relating to the security of customer data and accounts through a National Security Commitment as part of T-Mobile's merger with Sprint.

60. These outward facing statements are consistent with T-Mobile's duties under the Federal Communications Act of 1934 ("FCA") as well as other related statutes and regulations.

61. Despite these assurances and other similar statements, T-Mobile fails to provide reasonable and appropriate security sufficient to prevent unauthorized access

to customers' accounts, including those instances of unauthorized access by T-Mobile's employees, vendors, dealers, agents and representatives themselves.

62. Instead, T-Mobile tends to take the position in litigation that they are not paid enough to provide account security to their customers.

63. For example, upon information and belief, under the inadequate procedures negligently implemented by T-Mobile, unauthorized persons, including T-Mobile's own officers, agents, vendors, dealers and employees can easily authenticate, access, share, bypass security, and make changes to customers' information without customer permission using T-Mobile property such as the REMO devices.

64. In some instances, T-Mobile attempts to delegate responsibility for account security to third parties which use shared credentials, who may be located in or owned by parties in foreign countries, and who have unfettered access to customer accounts and data.

65. Defendant T-Mobile failed to disclose or made deceptive statements designed to cover up for the fact that it is aware that their security procedures can and do fall short of their expressed and implied representations and promises, as well as their statutory duties.

66. T-Mobile has been aware of the pervasive harm posed by SIM-swapping for years, doing little to actually address their unique and known vulnerabilities, notify their customers of the potential fallout of these unauthorized SIM-swaps, or protect

their customers from these SIM-swaps, including those performed by or with the assistance of T-Mobile's own employees, vendors, dealers and agents.

67. As Defendant T-Mobile is aware, an unauthorized SIM-swap can be particularly devastating because many internet services – including email, online banks (such as Defendant T-Mobile USA, Inc.'s own T-Mobile MONEY), and cryptocurrency exchanges, require and rely upon mobile phone numbers to help users recover and/or validate account access.

68. As a result of T-Mobile's misconduct as alleged herein, including gross negligence in protecting customer information, negligent hiring, training and supervision of customer support personnel, and violations of federal and state laws designed to protect wireless service consumers, Plaintiff had their cryptocurrency and other assets stolen. Said cryptocurrency had an estimated value at the time of loss of approximately $290,398.76.

69. This theft of Plaintiff's cryptocurrency was a direct result of the intentional actions, inaction and negligent practices of Respondent, including but not limited to their repeated failure to satisfy their duties to their customers under both federal and state laws.

70. As alleged herein, T-Mobile fragrantly and repeatedly violated its duties owed to Plaintiff in its Privacy Policy, COBC, Terms and Conditions, and CPNI Policy, as well as its legal obligations under the FCA, the CPNI Rules, the Red Flags Rule, and other laws, by willingly turning over Plaintiff's wireless number to an

unauthorized party, that then directly resulted in the third party gaining access to Plaintiff's information, account, cloud data, email and financial accounts.

71. Plaintiff therefore seeks compensatory, punitive, injunctive, declaratory and equitable relief restoring to them the assets, property and funds which were illegally taken from them.

c. SIM-swaps

72. A subscriber identity module, widely known as a "SIM card," stores user data in phones on the Global System for Mobile (GSM) network, the radio network used by Defendant T-Mobile USA, Inc. to provide cellular service to its subscribers.

73. SIM cards are principally used to authenticate cellphone subscriptions, as without a SIM card, GSM phones are not able to connect to T-Mobile's telecommunications network.

74. However, if placed in the wrong hands, a SIM card can also be used to steal someone's identity.

75. The FBI has stated that ""[o]nce the SIM is swapped, the victim's calls, texts, and other data are diverted to the criminal's device. This access allows criminals to send "Forgot Password" or "Account Recovery" requests to the victim's email and other online accounts associated with the victim's mobile telephone number." https://www.ic3.gov/Media/Y2022/PSA220208.

76. One of the most damaging and pervasive forms of account takeover fraud is known as a "SIM-Swap", whereby a party (with the help of a wireless carrier like

T-Mobile) is allowed to transfer access to a customer's cellular phone number from the customer's registered "subscriber identity module" card (or "SIM card") – to a SIM card controlled by that third party.

77. Sometimes these schemes are perpetrated by employees of the wireless carriers, such as T-Mobile.

78. Moreover, the wireless carrier must effectuate the SIM card reassignment and, therefore, "SIM-swapping" is not an isolated criminal act, as it requires the wireless carrier's active involvement to swap the SIM containing information regarding its customer to an unauthorized person's phone.

79. Indeed, unlike a direct hack of data, whereby a company like T-Mobile might play a more passive role, SIM-swaps are ultimately effectuated by the wireless carrier itself. For instance, in this case, it is T-Mobile that approved and allowed the SIM card change (without Plaintiff's authorization and without following their own policies/procedures), as well as all of the subsequent telecommunication activity that was used to access Plaintiff's online accounts and cause the injuries suffered by Plaintiff.

80. As such, by directly or indirectly exceeding the authorized access to customer accounts, wireless carriers such as T-Mobile may be liable under state and federal statutes, such as the Federal Communications Act ("FCA").

81. Once a third-party has access to the legitimate user's SIM card data, it can then seamlessly impersonate that customer (e.g., in communicating with others, requesting account access, downloading backup files, or contacting various vendors).

82. In some instances, the party now with control of the customer's account will then attempt to gain entry into the victim's email accounts by entering the victim's email address on Outlook, Yahoo, Gmail or any other email provider, selecting the "Forgot Password" option, and then receiving a text message intended for the account holder with a password reset code. Once inside the victim's email account, the thief then scours information stored on the victim's email account. The thief may also search for information from previous T-Mobile data breaches or data stored on a backup of information from the victim's wireless phone – which has been wirelessly delivered to them by T-Mobile – to find information such as passwords, previously downloaded applications, cloud data, or other identifying information that would grant the thief access into the victim's email, banking and investment accounts.

83. By using the victim's T-Mobile telephone number, the thief then may divert to themselves access to the victim's banking and investment accounts by using the victim's T-Mobile telephone number as a recovery or verification method.

84. A common target of SIM-swapping and account takeover fraud are individuals known or expected to hold cryptocurrency, because account information is often contained on users' cellular phones which allows criminals to transfer to legitimate user's cryptocurrency to an account the third-party controls.

85. SIM-swaps are not a new unforeseeable phenomenon, but instead have been discussed by federal authorities and telecommunications companies since at least 2016.

86. In June 2016, the FTC's then Chief Technologist, herself a victim of an account takeover, recounted her experience and offered advice to wireless carriers to help consumers avoid these takeover attacks, stating:

> "The mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking and fraudulent new accounts. In fact, many of them are obligated to comply with the Red Flags Rule, which, among other things, requires them to have a written identity theft prevention program. Carriers should adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions… [M]obile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss and having email, social network, and other accounts compromised."[1]

87. T-Mobile does not appear to adhere to that Red Flags Rule, as they do not seem to have a written identity theft prevention program in place that is available to and reviewed with their employees, agents, vendors and/or dealers.

[1] Lorrie Cranor, "Your mobile phone account could be hijacked by an identity thief," Tech@FTC (June 7, 2016), available at https://www.ftc.gov/. Mrs. Cranor also detailed her concerns about SIM-swapping in her reply comments before the FCC in July 2016. See In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunication Services, WC Docket No. 16-106 (July 6, 2016).

88. In a 2019 article about SIM-swapping that included multiple quotes from T-Mobile personnel, the New York Times reported that "[c]riminals have learned how to persuade mobile phone providers like T-Mobile and AT&T to switch a phone number to a new device that is under their control."[2]

89. Attention by both the media and government regulators, however, did not ensure that T-Mobile took security seriously enough to prevent account takeover accounts, to keep SIM-swapping schemes from increasing in prevalence on their network, to secure and prevent unauthorized use of employee/dealer/vendor credentials; to secure and prevent unauthorized access and use of T-Mobile REMO devices; or to convince themselves as a company to stop engaging in practices that violate their customers' rights and federal law.

90. For example, T-Mobile allows third-party vendors, dealers and retailers to access T-Mobile systems and customer accounts with limited or no protections in place to prevent unauthorized access.

91. These third party vendor/dealers often share login credentials, and T-Mobile has failed to take any effective measures to prevent these third party agents from gaining unauthorized access to customer accounts, selling that access, or directly robbing T-Mobile customers themselves.

[2] Nathaniel Popper, "Hackers Hit Twitter C.E.O. in a 'SIM-swap.' You're at Risk, Too," New York Times (September 5, 2019)

92. As such, in February of 2020, the FCC issued a "Notice of Apparent Liability for Forfeiture and Admonishment" proposing $91,630,000.00 penalty against T-Mobile for misuse of CPNI, where Commissioner Geoffrey Starks explained:

> Going forward, Americans must be able to place trust in their wireless carriers….[T]hese carriers know that the services they offer create risks for users: unauthorized location tracking, SIM hijacking, and billing scams to name just [a] few. Carriers must take responsibility for those people they allow into their operations.[3]

93. T-Mobile continues to refuse to take any significant or effective action in order to protect their customers from unauthorized SIM-swaps and misuse of CPI/CPNI, resulting in the FCC and Federal Trade Commission "receiv[ing] hundreds of consumer complaints about SIM-swapping" on a yearly basis.[4]

94. These complaints include instances where "the wireless carrier's store employees are involved in the fraud" or where "carriers completed SIM swaps despite the customer having previously set a PIN or password on the account." Id.

95. Since carriers like T-Mobile were not doing enough to protect customer accounts, CPI and CPNI, the FCC sought to strengthen their rules for wireless carriers dealing with SIM-swaps, and sought comment regarding the same.

---

[3] In the Matter of T-Mobile USA, Inc., File No. EB-TCD-18-00027708 (February 28, 2020).
[4] In the Matter of Protecting Consumers from SIM Swap and Port-Out Fraud, WC Docket No. 21-341 (September 30, 2021).

96. In response, T-Mobile resisted any implementation of restrictive additional safeguards for consumers, and instead engaged in a similar pattern of deferring both responsibility and blame for their own negligence towards their customers. For example, T-Mobile stated that "T-Mobile has policies in place to combat SIM swap and port-out fraud by empowering customers and deterring malicious actors, including account protection, monitoring, and rapid response to suspected fraud."[5]

97. At the same time, T-Mobile asserted that it already "has robust protections in place to help prevent fraudulent SIM swapping and port-outs from occurring." Id.

98. As such, despite the massive amounts of media, governmental, and academic focus on the issue of unauthorized SIM-swaps and the internal vulnerabilities of wireless carrier systems, T-Mobile has refused to institute the practices, procedures, and safeguards necessary to protect its customers' data from account takeover and SIM-swap attacks.

99. T-Mobile has failed to establish sufficient protections against numerous instances of T-Mobile's own employees, agents, and/or vendors either performing the unauthorized SIM-swaps themselves, or otherwise actively cooperating with hackers

[5] Comments of T-Mobile USA, Inc., In the Matter of Protecting Consumers from SIM Swap and Port-Out Fraud, WC Docket No. 21-341 (September 30, 2021).

in SIM-swaps by allowing direct access to customer information and/or by ignoring or overriding T-Mobile security procedures.

100. The full extent of this participation is known only to T-Mobile USA, Inc. and will need to be uncovered throughout the course of discovery. Upon information and belief, this participation includes, but is not limited to: employees/agents/vendors knowingly, recklessly and/or negligently accessing or providing access to customer accounts to individuals which they know, or should know, have no right to access those accounts; executives/managers/employees/agents/vendors taking steps to conceal the underlying facts of the SIM-swap or failing to alert the customer in a timely fashion of the occurrence of such an attack; executives/managers/employees/agents/vendors destroying or failing to preserve evidence they knew, or should have known, would be the subject of litigation and which would enable customers such as Plaintiff to track their stolen property and identify those responsible; executives/managers/employees/agents/vendors concealing the identifies of those responsible; executives/managers/employees/agents/vendors intentionally, negligently and/or recklessly failing to follow protocols and procedures ostensibly put in place by the FCC and Defendant in order to avoid these kinds of issues; hiding their role in these unauthorized SIM-swaps from their customers, the Secret Service, FBI, and FCC; and otherwise taking action or failing to take actions which perpetuate the theft of both property and identity.

101. The prevalence of SIM-swap fraud and T-Mobile's knowledge of such fraud, including but not limited to that performed with the active participation of its own employees (and the knowledge of its executives), demonstrate that what happened with Plaintiff's account was neither an isolated incident nor an unforeseeable event.

102. In light of the above, at the time of the events at issue in the present case, T-Mobile and their executives were uniquely and keenly aware of the company's obligations, as well as multiple weaknesses in T-Mobile's internal processes and procedures to authenticate legitimate customers, employees, agents and vendors.

103. Yet T-Mobile failed to prevent the unauthorized SIM-swap in this case (and many others), causing Plaintiff to lose a variety of assets, including cryptocurrency, with a value at the time of loss of approximately $290,398.76.

d. The January 23, 2022 SIM-swap

104. In the instant matter, on or around January 23, 2022, T-Mobile – whether acting as the thief, a co-conspirator to the theft or through abject negligence - transferred control of Plaintiff's T-Mobile account and telephone number using T-Mobile login credentials and a T-Mobile device to an unauthorized third party, which led to the almost immediate theft of more than $290,429.12 in property, including cryptocurrency assets, from Plaintiff.

105. On or around January 23, 2022, without properly following the mandates of Section 222 of the FCA and/or internal policies and procedures, T-Mobile

transferred control of Plaintiff's account and telephone number through an unauthorized SIM-swap to an unauthorized individual, disconnecting the telephone number from Plaintiff's wireless phone's SIM card and connecting the telephone number to a SIM-card under the control of the unauthorized individual.

106. Utilizing T-Mobile's own systems and applications, and a vendor/dealer login code, the third party would have been presented with Plaintiff's account details, including his name, address, contact information, email addresses, social security numbers, pin numbers, passwords, credit information and more.

107. Upon logging into their cryptocurrency account(s) on or around that day, Plaintiff saw that their cryptocurrency wallet(s) and account(s) at major cryptocurrency exchanges had been compromised.

108. Defendant T-Mobile would not confirm a SIM-swap had occurred on Plaintiff's account until sending him a letter in the mail almost 2 months later, on or around March 7, 2022.

109. In that letter, T-Mobile sated that they had "detected unauthorized activity on your T-Mobile account, during which an unknown party would have had access to [CPNI]….Specifically, an unknown party assigned your phone line(s)…to the SIM card in a device other than yours on 1/23/2022…."

110. Despite what T-Mobile intentionally misrepresented to Plaintiff via that letter, it was not an "unknown party" that "assigned [Plaintiff's] phone line(s)…to [a

different] SIM card", but was instead a T-Mobile employee, agent, dealer and/or vendor who assigned Plaintiff's phone line to a different SIM card.

111. As a direct and proximate result of T-Mobile's acts and omissions, the following property was stolen from Plaintiff on or around January 23, 2022:

Date of Theft	**Location From Which Assets Were Stolen**	**Cryptocurrency / Assets Stolen**	**Approximate Value of Funds / Assets Stolen**
Jan. 23, 2022	Coinbase	4.69126943 BTC	$170,918.47
Jan. 23, 2022	Coinbase	109.507 SOL	$11,433.63
Jan. 23, 2022	Coinbase	200290 ASM	$12,033.42
Jan. 23, 2022	Coinbase	96179.2 ARPA	$5,613.98
Jan. 23, 2022	Coinbase	26185.6 NKN	$5,323.53
Jan. 23, 2022	Coinbase	22,49715677 ETH	$57,190.92
Jan. 23, 2022	Binance	.58568573 BTC	$21,338.48
Jan. 23, 2022	BSC Token Hub	5.302 BNB	$2,060.30
Jan. 23, 2022	MetaMask	190570487.504590710777649276 SHIB	$4,486.03
		TOTAL	**$290,398.76**

112. The theft from Plaintiff would not have occurred but for T-Mobile's failure to adequately protect Plaintiff's T-Mobile account, T-Mobile employee/vendor credentials, T-Mobile property including REMO devices, and otherwise to maintain

and enforce proper security measures to prevent the unauthorized SIM-swap(s) that took place.

113. Through its procedures, practices, and action/inaction, T-Mobile engages in behavior which fails to provide reasonable, appropriate, and required security to prevent unauthorized access to their customers' wireless accounts, allowing persons to be improperly granted access to sensitive customer wireless account data.

114. In January of 2022, Plaintiff was a wireless customer of T-Mobile, and had placed an additional level of security onto his account through means of a PIN.

115. At that time, Plaintiff was holding cryptocurrency for personal use and investment in cryptocurrency wallets and/or exchanges -- digital currency wallet(s) and online platform(s) to transfer and store digital currency.

116. Plaintiff entrusted his sensitive private information to T-Mobile, and reasonably relied on T-Mobile's assurances of and its stated compliance with applicable laws, including (but not limited to) the FCA and the Red Flags Rule.

117. Instead, Plaintiff was a victim of an unauthorized SIM-swap and theft that was, if not entirely perpetrated by T-Mobile, then at the very least effectuated and facilitated by T-Mobile and their policies, procedures, employees, agents and/or vendors.

118. Plaintiff did not authorize T-Mobile or anyone else to use, disclose, share, or access his account, CPI and/or CPNI that was maintained by T-Mobile.

119. To the contrary, Plaintiff had an objectively reasonable expectation and a fundamental right to conduct his personal activities without observation, intrusion or interference.

120. Therefore, any use, disclosure or access to Plaintiff's account, CPI and/or CPNI on or around January 23, 2022 was unauthorized, unlawful, and caused by T-Mobile's employees, agents, vendors, policies and/or procedures.

121. To the best of Plaintiff's knowledge, information and belief, T-Mobile knows the identity of those entities and individuals working for or on behalf of T-Mobile who participated in the actions complained of herein.

122. This is in direct contravention to the misrepresentations made by T-Mobile to Plaintiff on or around March 7, 2022 that they do not know the identity of the person within T-Mobile who assigned Plaintiff's phone line to a different SIM-card.

123. Since that time, on multiple occasions, Plaintiff has requested information from T-Mobile regarding the facts surrounding the theft of his property, and the identities of those individuals who participated in the theft.

124. To date, T-Mobile USA, Inc. has affirmatively refused to provide any substantive information relating to the facts surrounding the theft of Plaintiff's property.

125. That information is solely in the possession, custody and/or control of T-Mobile USA, Inc.

126. Upon information and belief, T-Mobile USA, Inc. has intentionally failed to preserve evidence relating to the theft of Plaintiff's property, or has taken steps to conceal those facts relating to the participation of T-Mobile in the theft of Plaintiff's property.

127. T-Mobile, despite having a legal obligation to do so, abjectly failed in its duty to safeguard their customers' personal and financial information by providing unauthorized access to Plaintiff's account, CPI and/or CPNI.

128. T-Mobile failed to implement, follow, and/or maintain security policies and procedures, including the written identity theft program required under the Red Flags Rule, sufficient to protect their customers' accounts, CPI and/or CPNI from unauthorized access.

129. T-Mobile failed to properly and sufficiently hire, train, supervise and/or discipline their employees, agents and/or vendors in order to prevent unauthorized access to Plaintiff's account, information, CPI and/or CPNI.

130. T-Mobile could have reasonably foreseen the consequences of failing in its duty to implement, maintain, and execute sufficient security policies and practices to protect the unauthorized access to consumer data, including that of Plaintiff.

131. T-Mobile's systems, policies, and procedures allow its officers, agents, and employees to exceed the authorized access to customers' accounts without permission or justification, or otherwise allow their credentials to be used for the same.

132. T-Mobile's actions and inaction demonstrate a reckless disregard for the rights of its customers and those with whom its customers deal (i.e., other foreseeable victims).

133. T-Mobile's actions and inaction also demonstrate a reckless disregard for its obligations, responsibilities, and duties under the law.

134. The damage suffered by Plaintiff is directly related to the wrongful conduct of allowing the unauthorized access to Plaintiff's wireless account.

135. Indeed, but for T-Mobile's reckless disregard of their obligations, Plaintiff would not have been damaged.

136. By its procedures, policies and practices, T-Mobile engages in behavior that fails to provide reasonable, necessary, and appropriate security to prevent or respond to unauthorized access to their customers' wireless accounts, permitting unauthorized persons to gain access to sensitive customer wireless accounts and data.

137. T-Mobile:

a. Failed to establish or enforce rules sufficient to ensure that only authorized persons have access to T-Mobile customer accounts;
b. Failed to establish or enforce appropriate rules, policies or procedures for the supervision, hiring, control and/or discipline of its officers, employees, agents or vendors and/or their credentials;
c. Failed to establish or enforce rules, or provide adequate supervision, hiring, training or discipline sufficient to ensure that all of their officers, employees, agents and vendors are

knowledgeable of and adhere to the same policies and procedures. For example, most third-party agents, dealers and vendors are untrained and/or unaware of T-Mobile policies and procedures (such as the written identity theft program required under the Red Flags Rule), which are arguably supposed to cover their conduct, and often are not subjected to purportedly mandatory background checks and training;

d. Failed to adequately safeguard and protect their customers' wireless accounts, including that of Plaintiff, T-Mobile credentials, or T-Mobile property, so unauthorized people were able to gain access to Plaintiff's accounts and information;

e. Permitted the sharing of and access to user credentials among T-Mobile's employees, agents and vendors thus reducing likely detection of, and accountability for, unauthorized access;

f. Loosened their internal security protocols requiring authentication of T-Mobile employees, agents, and vendors which directly led to an increase in the number of unknown and untraceable parties gaining improper access to T-Mobile customer information;

g. Knowingly leaves tablets/iPads unprotected and unsecured in T-Mobile stores which, if stolen, grants unfettered access to any and all T-Mobile customer accounts without a need for authentication;

h. Failed to adequately train, hire, supervise and/or discipline their employees, agents and/or vendors, allowing those individuals to unilaterally access and make unauthorized changes to customer accounts;

i. Allowed porting out of phone numbers without properly confirming that the request was coming from legitimate customers or dealers by, for example, checking that the location of the requester matches readily available information on file;

j. Lacked proper monitoring systems and thus is unable to detect unauthorized access to customer accounts or employee information, so that the breach of security and diversion of customer information was able to occur in Plaintiff's situation and continued until after Plaintiff's virtual currency accounts were compromised;

k. Failed to implement simple, low-cost, and readily available defenses to identity thieves, such as delaying changes to accounts to allow for additional verifications from the customer and/or agent;

l. Failed to build adequate internal tools to help protect the customers and against hackers and account takeovers, including protection from phone porting and wrongdoing by its own agents or employees acting on their behalf or on behalf of or at the request of a third-party;

m. Failed to notify Plaintiff of changes to their account or T-Mobile's Terms and Conditions in a prompt manner; and

n. Failed to notify law enforcement of purportedly criminal activity.

138. As such, T-Mobile's security measures were and are entirely inadequate to protect their customers such as Plaintiff, and the user/employee/agent/vendor verification/credential structures created an unreasonable and foreseeable risk of unauthorized access to customer accounts, including that of Plaintiff.

139. Upon information and belief, T-Mobile and its officers have long been aware of the security risks presented by, *inter alia*, their weak user/employee/agent/vendor verification/credential structures and procedures. In fact, T-Mobile has taken affirmative steps to *reduce* their verification procedures, and to this day does not use readily available security measures, such as those used by its competitors, to prevent or limit unauthorized access to their customer accounts/CPI/CPNI.

140. As such, T-Mobile has failed in their regulatory obligations and the duties they owed to Plaintiff to protect his account, information, CPI, and CPNI.

141. Even if the subject incident was due to an "inside" job or human performance falling short, T-Mobile is responsible for their employees, agents and vendors.

142. While T-Mobile may outsource customer service functions, such as to vendors in other countries, T-Mobile cannot transfer accountability under state and federal statutes.

143. Had T-Mobile provided adequate account security, exercised reasonable oversight of their employees/agents/vendors and property, or complied with their statutory duties, Plaintiff would not have lost his phone number or otherwise been damaged.

144. As a result of the foregoing acts, errors and omissions by T-Mobile, Plaintiff has been damaged in an amount that will be proven at any ultimate hearing or trial.

145. Plaintiff has fully performed all of his duties and obligations, and any conditions precedent to Plaintiff bringing this action have been performed, or else have been excused or waived.

146. To enforce his rights, Plaintiff has retained undersigned counsel and is obligated to pay counsel a reasonable fee for its services, for which T-Mobile is liable under federal and state statutes, as well as their own Terms and Conditions.

147. To enforce his rights, Plaintiff has been forced and will in the future continue to be forced to expend money for costs, taxes and fees related to the arbitration and litigation of his claims, for which T-Mobile is liable under federal and state statutes, as well as their own Terms and Conditions.

V. CAUSES OF ACTION

COUNT I
Violation(s) of the California Arbitration Act ("CAA")

148. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

149. Cal. Code Civ. Proc. § 1281.98(a)(1) states that: "In an employment or consumer arbitration that requires, either expressly or through application of state or federal law or the rules of the arbitration provider, that the drafting party pay certain fees and costs during the pendency of an arbitration proceeding, if the fees or costs

required to continue the arbitration proceeding are not paid within 30 days after the due date, the drafting party is in material breach of the arbitration agreement, is in default of the arbitration, and waives its right to compel the employee or consumer to proceed with that arbitration as a result of the material breach."

150. Cal. Code Civ. Proc. § 1281.98(b)(1) provides that:

> "If the drafting party materially breaches the arbitration agreement and is in default under subdivision (a), the employee or consumer may unilaterally elect to do any of the following: (1) Withdraw the claim from arbitration and proceed in a court of appropriate jurisdiction. If the employee or consumer withdraws the claim from arbitration and proceeds with an action in a court of appropriate jurisdiction, the statute of limitations with regard to all claims brought or that relate back to any claim brought in arbitration shall be tolled as of the date of the first filing of a claim in any court, arbitration forum, or other dispute resolution forum."

151. Cal. Code Civ. Proc. § 1281.98(c) states that:

> "If the employee or consumer withdraws the claim from arbitration and proceeds in a court of appropriate jurisdiction pursuant to paragraph (1) of subdivision (b), both of the following apply:
>
> (1) The employee or consumer may bring a motion, or a separate action, to recover all attorneys' fees and all costs associated with the abandoned arbitration proceeding. The recovery of arbitration fees, interest, and related attorneys' fees

shall be without regard to any findings on the merits in the underlying action or arbitration."

(2) The court shall impose sanctions on the drafting party in accordance with Section 1281.99.

152. Cal. Code Civ. Proc. § 1281.99(a) states that: "The court shall impose a monetary sanction against a drafting party that materially breaches an arbitration agreement pursuant to subdivision (a) of Section 1281.97 or subdivision (a) of Section 1281.98, by ordering the drafting party to pay the reasonable expenses, including attorney's fees and costs, incurred by the employee or consumer as a result of the material breach."

153. Cal. Code Civ. Proc. § 1281.99(b) provides that: "In addition to the monetary sanction described in subdivision (a), the court may order any of the following sanctions against a drafting party that materially breaches an arbitration agreement pursuant to subdivision (a) of Section 1281.97 or subdivision (a) of Section 1281.98, unless the court finds that the one subject to the sanction acted with substantial justification or that other circumstances make the imposition of the sanction unjust.

(1) An evidence sanction by an order prohibiting the drafting party from conducting discovery in the civil action.

(2) A terminating sanction by one of the following orders:

a. An order striking out the pleadings or parts of the pleadings of the drafting party.

b. An order rendering a judgment by default against the drafting party.

(3) A contempt sanction by an order treating the drafting party as in contempt of court.

154. On or around August 23, 2022 Plaintiff filed a Demand for Consumer Arbitration and a detailed Statement of Claims against T-Mobile USA, Inc. with the American Arbitration Association ("AAA") under a set of Terms and Conditions drafted by Defendant T-Mobile USA, Inc.

155. In order to initiate that arbitration proceeding, Plaintiff paid a filing fee to the AAA, attorneys' fees to his counsel, and certain costs associated with that proceeding.

156. Before the AAA would continue that arbitration between Plaintiff and Defendant, the AAA required Defendant T-Mobile USA, Inc. to pay certain fees and costs.

157. Additionally, under T-Mobile USA, Inc.'s Terms and Conditions, immediately upon payment of the filing fees by Plaintiff, Defendant was required to reimburse Plaintiff those filing fees.

158. Defendant T-Mobile USA, Inc. was given 30 days and multiple warnings regarding the payment of those fees and costs.

159. Defendant T-Mobile USA, Inc. failed to pay those fees and costs, which is a material breach of their Terms and Conditions, the rules of the AAA, and the CAA.

160. As a result of Defendant T-Mobile USA, Inc.'s material breaches and violations of the CAA, Plaintiff was forced to needlessly expend resources and time.

161. T-Mobile's default stance in arbitration proceedings is that their customers have no right to bring claims against T-Mobile USA, Inc., and that their customers have no right to seek damages against T-Mobile USA, Inc. T-Mobile USA, Inc. regularly seeks to dismiss their customers' claims in arbitration, currently opposes reimbursement of fees/costs, seeks attorneys' fees in contravention of their Terms and Conditions, and engages in severely limited discovery including refusing to provide or permit third party discovery which prejudices the rights of their customers in arbitration.

162. Accordingly, Plaintiff withdrew his claims from arbitration and now seeks to proceed with an action in this Court.

163. As part of this action, Plaintiff seeks recovery of all arbitration fees, attorneys' fees, costs, expenses, other fees and the interest on the same.

164. Additionally, due to T-Mobile USA, Inc's material breaches and violations of the CAA, Plaintiff seeks monetary sanctions against T-Mobile USA, Inc. in an amount sufficient to cover all attorneys' fees, costs, expenses, expert witness fees, local counsel fees, and any other money Plaintiff expends or is charged preparing for, filing and proceeding with this litigation

165. Plaintiff also seeks sanctions against Defendant T-Mobile USA, Inc. under Cal. Code Civ. Proc. § 1281.99(b) seeking: (1) to prohibit T-Mobile USA, Inc. from conducting discovery in this action; (2) an order striking T-Mobile USA, Inc.'s pleadings in this action; (3) an order rendering a judgment by default against T-Mobile

USA, Inc.; and (4) a contempt sanction against T-Mobile USA, Inc. treating Defendant as in contempt of court.

COUNT II
Violation(s) of the California Unfair Competition Law ("UCL")

166. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

167. California's Unfair Competition Law ("UCL"), California Business & Professional Code § 17200, prohibits any "unlawful, unfair or fraudulent business act or practice." T-Mobile's business acts and practices complained of herein were unlawful, unfair and fraudulent.

168. T-Mobile USA, Inc. made material misrepresentations and omissions concerning its safeguarding of Plaintiff's account, CPI and CPNI. A reasonable person would attach importance to the privacy of their sensitive account data in determining whether to contract with a mobile phone provider.

169. T-Mobile USA, Inc. had a duty to disclose the nature of their inadequate security practices, the extensive number of data breaches and unauthorized SIM-swaps suffered by their customers, the impact of those breaches, the role of their agents and property in those breaches, and T-Mobile's failures in hiring, training and supervising staffing. T-Mobile had exclusive knowledge of material facts not known or knowable to T-Mobile customers, including Plaintiff, and T-Mobile actively concealed these material facts from their customers, including Plaintiff.

170. Further, additional disclosures were necessary to materially qualify T-Mobile's representations that it took measures to protect customer data, and its partial disclosures concerning its use of customers' CPNI. T-Mobile was obligated to disclose its practices by the FCA. The magnitude of harm suffered by Plaintiff underscores the materiality of T-Mobile's omissions and misrepresentations.

171. A reasonable person, such as Plaintiff, would be deceived and misled by T-Mobile's misrepresentations, which indicated that T-Mobile would safeguard their customers' personal and proprietary information.

172. T-Mobile intentionally misled its customers regarding its data protection practices in order to attract customers and evade prosecution for its unlawful acts.

173. For instance, T-Mobile USA, Inc. would represent to their customers and potential customers that their accounts were safe and secure, while simultaneously making surreptitious edits to the middle of a paragraph 22 pages deep into their unpaginated Terms and Conditions in an attempt to limit their liability to their customers for financial and cryptocurrency losses suffered as a result of T-Mobile's lackadaisical security practices. Said edit makes no contextual sense to T-Mobile customers, who may never have been presented with, seen, reviewed, or understood those terms, without the knowledge exclusively in T-Mobile's possession.

174. T-Mobile's Terms and Conditions themselves also represent an unfair and unlawful business act or practice where within the first few pages they represent to their customers and potential customers that they can seek and pursue the same

causes of action and damages through arbitration as they could in a court of law, but then some 20 pages deep into those Terms and Conditions they attempt to limit their customers' ability to pursue *any* damages or claims against T-Mobile USA, Inc.

175. T-Mobile's actions detailed herein constitute an unlawful business act or practice.

176. As alleged herein, T-Mobile's conduct is also a violation of the California constitutional right to privacy, the FCA, the Red Flags Rule, and other rules, regulations and statutes.

177. T-Mobile's conduct lacks reasonable and/or legitimate justification in that Plaintiff has been misled as to the nature and integrity of T-Mobile's goods and services and has suffered significant damages as a result.

178. T-Mobile's practices are contrary to the requirements of the FCA and its corresponding regulations, which require mobile carriers to disclose customers' CPNI only upon proper notice, consent and authorization, and aims to vest customers with control over their data. Due to the nature of T-Mobile's actions, including the role played by T-Mobile agents and T-Mobile property, Plaintiff could not have reasonably avoided the harms incurred.

179. As the FCA establishes, it is against public policy to allow carrier employees or other third parties to access, use, or disclose telecommunications customers' sensitive account information. The effects of T-Mobile's conduct are comparable to or the same as a violation of the FCA.

180. T-Mobile's actions detailed herein constitute a fraudulent business act or practice.

181. As averred herein, Plaintiff has suffered significant damages as a result of T-Mobile's unfair competition. Had T-Mobile disclosed the true nature and extent of their data security and protection practices – and the flaws inherent in their policies, practices and systems – and their repeated failure to properly protect their customers – Plaintiff would not have subscribed to or paid money to T-Mobile for their mobile services.

182. Plaintiff seeks damages, injunctive and declaratory relief for T-Mobile's violations of the UCL. Plaintiff further seeks public injunctive relief against T-Mobile's unfair and unlawful practices in order to protect the public and restore to the parties in interest money or property taken as a result of T-Mobile's unfair competition and deceptive business practices. Plaintiff also seeks a mandatory cessation of and revisions to T-Mobile's practices, proper safeguarding of T-Mobile account data, and significant changes to T-Mobile's Terms and Conditions and the written identity theft program required under the Red Flags Rule.

COUNT III
Violation(s) of the Federal Communications Act ("FCA")

183. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

184. The FCA regulates interstate telecommunications carriers, including T-Mobile.

185. T-Mobile is a "common carrier" or a "telecommunications carrier" engaged in interstate commerce by wire for the purpose of furnishing communication services within the meaning of Section 201(a) of the FCA. 47 U.S.C. § 201(a).

186. As a "common carrier" T-Mobile is subject to the substantive requirements of Sections 201 through 222 of the FCA. See 47 U.S.C. §§ 201-222.

187. Under Section 201(b) of the FCA, common carriers may implement only those practices, classifications, and regulations that are "just and reasonable" and practices that are "unjust or unreasonable" are unlawful.47 U.S.C. § 201(b).

188. Section 206 of the FCA, entitled "Carriers' liability for damages" provides:

> In case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney's fee, to be fixed by the court in every case of recovery, which attorney's fee shall be taxed and collected as a part of the costs in the case.

189. Section 207 of the FCA, entitled "Recovery of damages" further provides:

> Any person claiming to be damaged by any common carrier subject to the provisions of this chapter may either make

> complaint to the FCC as hereinafter provided for, or may bring suit for the recovery of the damages for which such common carrier may be liable under the provisions of this chapter, in any district court of the United States of competent jurisdiction….

190. Section 222(a) of the FCA provides that a telecommunications carrier has a duty to protect the confidentiality of the proprietary information of their customers. 47 U.S.C. § 222(a).

191. Additionally, Section 222(c) of the FCA explicitly requires that telecommunications carriers protect their customers' CPNI. 47 U.S.C. § 222(c).

192. According to the CPNI Rules:

> Safeguarding CPNI. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated contact, online account access, or an in-store visit.
>
> …
>
> In-store access to CPNI. A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.[6]

[6] 47 C.F.R. §64.2010(a), (d). For purposes of the CPNI Rules, the term "customer" means "[a] person…to which the telecommunications carrier is currently providing service," while the term "valid photo ID" means "a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired." 47 C.F.R. §64.2004(f), (r).

193. T-Mobile violated its duties under Section 222 of the FCA and the CPNI Rules by failing to protect Plaintiff's CPI and CPNI by using, disclosing, or permitting access to Plaintiff's account, information, CPI and CPNI without the consent of, notice to, and/or legal authorization by Plaintiff as required by the FCA, in that upon information and belief:

a. A T-Mobile employee, representative or agent used their credentials or allowed their credentials to be used in order to access and utilize Plaintiff's account, information, CPI and CPNI for the purpose of stealing from Plaintiff or to engage in a conspiracy to steal from Plaintiff;
b. Plaintiff's CPI and CPNI were disclosed to someone other than Plaintiff by an agent of T-Mobile;
c. Plaintiff's CPI and CPNI were disclosed to someone who was not properly authenticated by T-Mobile;
d. Plaintiff's CPI and CPNI were disclosed to someone who did not first present a valid photo ID to T-Mobile; and/or
e. Plaintiff's CPI and CPNI were disclosed to someone who did not match any of Plaintiff's account information or the T-Mobile employee/vendor/dealer/agent information of which T-Mobile was aware.

194. As alleged herein, T-Mobile failed to protect the confidentiality of Plaintiff's account, information, CPI and CPNI when it disclosed Plaintiff's account, information, CPI and CPNI to third-parties without Plaintiff's authorization or permission.

195. T-Mobile's conduct, as alleged herein and as will be established at any ultimate hearing in this matter, constitutes knowing violations of the FCA, including sections 201(b) and 222, as well as the CPNI Rules and Implementing Regulations.

196. T-Mobile is also liable for the acts, omissions, and/or failures, as alleged herein, of its officers, employees, agents, or any other persons acting for or on behalf of T-Mobile.

197. T-Mobile's violation of the FCA allowed unauthorized parties to impersonate Plaintiff in transactions with others, including Plaintiff's email and cryptocurrency account providers.

198. T-Mobile violated the FCA, including Section 222, by allowing an unauthorized party to access Plaintiff's CPI and CPNI, resulting in, *inter alia*, Plaintiff's loss of their property, including cryptocurrency with a value at time of loss in excess of $290,429.12.

199. As a direct consequence of T-Mobile's violations of the FCA, Plaintiff has been damaged through the loss of his property and other associated damages.

200. Had T-Mobile not allowed the unauthorized access to Plaintiff's account, Plaintiff would not have suffered this loss.

201. T-Mobile, by its inadequate procedures, practices, and policies, engages in behavior which:

a. Fails to provide reasonable, appropriate, and sufficient security to prevent unauthorized access to its customers' wireless accounts, CPI and CPNI;

b. Allows unauthorized persons to be authenticated or to bypass authentication; and

c. Grants improper access to sensitive customer account information.

202. In particular, T-Mobile failed to establish and implement reasonable policies, procedures and safeguards governing the creation, access, and authentication of user credentials and T-Mobile REMO devices to access customers' accounts, creating an unreasonable and foreseeable risk of unauthorized access.

203. As such, in violation of the FCA, T-Mobile has failed to ensure that only authorized persons have access to customer account data and that customers' accounts, CPI and CPNI are secure.

204. Among other things, T-Mobile:

a. Failed to establish and enforce rules and procedures sufficient to ensure only authorized persons have access to T-Mobile customer accounts and information, including that of Plaintiff;

b. Failed to establish and enforce appropriate rules, standards, policies and procedures for the supervision, training, hiring, control and discipline of its officers, employees, agents and/or vendors;

c. Failed to establish and enforce rules, policies and procedures, including a written identity theft program under the Red Flags Rule, or to provide adequate supervision or training sufficient to ensure that its employees, agents and/or vendors are aware of and follow such rules, policies and procedures, in order to prevent access to customer accounts by unauthorized persons;

d. Failed to establish and enforce rules and procedures to ensure T-Mobile's employees and agents adhere to the security instructions of customers with regards to accessing customers' accounts, including that of Plaintiff, and that they cannot improperly bypass the same;

e. Failed to adequately safeguard and protect its customers' wireless accounts;

f. Permitted the sharing of and access to user credentials among T-Mobile's agents or employees, reducing the likely detection of and accountability for unauthorized access;

g. Failed to appropriately supervise employees, agents and/or vendors, who gained or granted unauthorized access to customers' accounts, including that of Plaintiff, seemingly in an effort to avoid liability and make obtaining redress by their customers as onerous as possible;

h. Failed to adequately train and supervise its employees, officers, agents and vendors to prevent unauthorized access to customer accounts;

i. Failed to prevent the ability of employees, officers, agents and vendors to access and make changes to customer accounts without specific customer authorization;

j. Allowed "porting out" of cell phone numbers without properly confirming that the request was coming from legitimate customers or T-Mobile employees, agents, officers and/or vendors;

k. Lacked proper monitoring and, therefore, failed to monitor its systems for the presence of unauthorized access in a manner that would allow T-Mobile to detect, prevent or address intrusions,

breaches of security, and unauthorized access to customer information in a timely manner;

l. Failed to implement and maintain readily available best practices to safeguard customer information (and indeed, seemed to suggest such practices were only available to those customers who "paid for" the privilege of having their information secured);

m. Failed to timely prevent, address, communicate, diagnose and/or determine the cause of Plaintiff's service interruption;

n. Failed to timely notify Plaintiff of the cause of Plaintiff's service interruption; and

o. Failed to implement and maintain internal controls to help protect against account takeovers and SIM-swaps by unauthorized persons.

205. The inadequate security measures, policies and safeguards employed by T-Mobile created a foreseeable and unreasonable risk of unauthorized access to the accounts of its customers, including that of Plaintiff.

206. Upon information and belief, T-Mobile has long been aware of its inadequate security measures, policies and safeguards, and nevertheless, induced customers into believing that its systems were secure and compliant with applicable law.

207. T-Mobile, despite knowing the risks associated with unauthorized access to customer accounts, failed to utilize reasonable and available methods to prevent or limit such unauthorized access, including that perpetrated using T-Mobile credentials

and property such as the REMO devices which are often left unattended and unprotected in their stores.

208. T-Mobile failed in its duty to protect and safeguard customer information and data pursuant to federal law.

209. Had T-Mobile implemented appropriate and reasonable security measures, Plaintiff would not have been damaged.

210. In sum, T-Mobile's security measures and the actions of their employees, agents and vendors were entirely inadequate to prevent the foreseeable damage caused to Plaintiff.

COUNT IV
Negligence

211. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

212. T-Mobile owes a duty of care to its customers to ensure the privacy and confidentiality of customer accounts, CPI and CPNI during its provision of wireless carrier services, as required by both federal and state law.

213. By allowing unauthorized access to the personal and confidential information of Plaintiff, T-Mobile breached their duties of care as owed to foreseeable victims, including Plaintiff.

214. By failing to prevent the unauthorized use of T-Mobile credentials and T-Mobile property, T-Mobile breached its duty of care to its customers and to foreseeable victims, including Plaintiff.

215. By failing to follow the Red Flags Rule, and by failing to implement, update, maintain and disseminate a written identity theft program, T-Mobile violations the laws and breached its duty of care to its customers and to foreseeable victims, including Plaintiff.

216. By failing to properly diagnose and notify Plaintiff of the cause of Plaintiff's service interruption in a timely fashion, T-Mobile breached its duty of care to Plaintiff.

217. By failing to notify Plaintiff of the risks of unauthorized SIM-swaps, data breaches, and the potential impact on financial and cryptocurrency accounts, T-Mobile breached its duty of care to Plaintiff.

218. By failing to implement, update, maintain and disseminate sufficient and effective protocols, policies, practices and procedures to protect customer data, including Plaintiff's private and confidential information, T-Mobile breached its duty of care to its customers and to foreseeable victims, including Plaintiff.

219. But for the inadequate security protocols, practices, and procedures employed by T-Mobile in protecting customer data, including preventing and addressing the breaches of Plaintiff's private and confidential information, Plaintiff would not have suffered any damages.

220. But for the inadequate protocols, practices, and procedures employed by T-Mobile in preventing, addressing, and diagnosing the causes of customers' service interruptions, Plaintiff would not have suffered any damages.

221. But for those intentional actions and/or inaction of T-Mobile and its agents, Plaintiff would not have suffered any damages.

222. And but for T-Mobile's inability to prevent, or quickly and effectively diagnose and/or determine that Plaintiff's account was compromised by an unauthorized SIM-swap – a fact that T-Mobile should have known – Plaintiff would not have suffered damages.

223. Plaintiff has been damaged through the loss of their property as described herein and as will be established at any ultimate hearing or trial.

COUNT V
Negligent Hiring, Retention, Training and Supervision

224. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

225. At all material times herein, T-Mobile's agents, officers, employees, dealers and vendors, including but not limited to those directly or indirectly responsible for or involved in allowing unauthorized access to Plaintiff's confidential and proprietary account information, were under T-Mobile's direct supervision and control.

226. Upon information and belief, T-Mobile negligently hired, retained, controlled, trained and supervised the officers, agents, employees, dealers and vendors under its control, or knew or should have known that such officers, agents, employees, dealers and vendors could gain or allow unauthorized access to customer accounts, including that of Plaintiff.

227. Upon information and belief, T-Mobile negligently failed to implement systems and procedures necessary to prevent its officers, agents, employees, dealers and vendors from allowing or obtaining unauthorized access to customer accounts, including that of Plaintiff, through among other things, the use of T-Mobile credentials and T-Mobile property.

228. Upon information and belief, T-Mobile's negligent hiring, retention, control, training and supervision allowed and/or facilitated the unauthorized access to customers' accounts resulting in damage to Plaintiff.

229. Given T-Mobile's experience with account takeover and SIM-swap attacks (including many perpetrated and/or assisted by T-Mobile's own employees, officers, vendors, dealers or agents), T-Mobile's failure to exercise reasonable care in screening, supervising, training, hiring and controlling its officers, agents, vendors, dealers and employees was a breach of its duty to Plaintiff.

230. T-Mobile's duty to its customers and foreseeable victims to protect its customers' data from unauthorized access is required by federal and state law.

231. It was entirely foreseeable to T-Mobile that unauthorized persons would attempt to gain unauthorized access to T-Mobile customers' data, including through the use of T-Mobile credentials and property, and, despite this, T-Mobile failed to implement sufficient safeguards and procedures to prevent its officers, agents, vendors, dealers and employees from granting, obtaining and/or facilitating such unauthorized access.

232. Upon information and belief, T-Mobile engaged in the acts alleged herein and/or condoned, permitted, authorized and/or ratified the conduct of its officers, agents, vendors, dealers and employees.

233. As a direct consequence of T-Mobile's negligent hiring, training, retention, control and supervision of its officers, agent, vendors, dealers and employees, who enabled or obtained the unauthorized access to Plaintiff's account, Plaintiff was damaged through the loss of their property as described herein and as will be established at any ultimate hearing or trial.

COUNT VI
Gross Negligence

234. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

235. T-Mobile, as required by federal and state law, owed Plaintiff a duty to properly handle and safeguard Plaintiff's account, information, CPI and CPNI and access to their account.

236. T-Mobile was required to ensure and certify its compliance with federal law and to protect the confidentiality of its customers' account data, including that of Plaintiff.

237. Upon information and belief, T-Mobile willfully disregarded and/or showed reckless indifference to its duties under federal and state law to T-Mobile customers and to foreseeable victims of T-Mobile's wrongful acts, including Plaintiff.

238. Having superior knowledge of prior account takeover attacks on T-Mobile customers' data and having the ability to employ internal systems, procedures, and safeguards to prevent such attacks, T-Mobile nevertheless failed as alleged throughout this Complaint, including:

a. Failed to institute appropriate controls to prevent unauthorized access to customers' accounts;

b. Utilized authentication systems it knew or should have known were vulnerable to account takeover attacks and/or removed authentication systems in the name of expedience over security;

c. Willfully disregarded the best practices of the industry in failing to implement systems to diagnose, prevent and/or thwart such attacks;

d. Failed to appropriately hire, retain, supervise, train and control those officers, agents, vendors, dealers and employees who could grant or obtain unauthorized access to customer account data;

e. Failed to implement and make accessible to employees/agents the written identity theft program required under the Red Flags Rule, or otherwise comply with that and other statutes/rules/regulations; and

f. Failed to secure and prevent the unauthorized use of employee/agent credentials, T-Mobile systems and T-Mobile property including REMO devices.

239. T-Mobile's policies, procedures and safeguards were completely ineffective and inadequate to diagnose, prevent or address unauthorized access to its customers' data.

240. T-Mobile's actions as alleged herein, in the face of an abundance of attention by the media and government regulators, as well as multiple pieces of litigation filed against them, evidence a carelessness that can only be characterized as a complete disregard for the rights of its customers and the foreseeable victims of its inadequate data security measures, including Plaintiff.

241. As a consequence of T-Mobile's gross negligence, Plaintiff has been damaged through the loss of his property as described herein and as will be established at any ultimate hearing or trial.

COUNT VII
Violation(s) of the Stored Communications Act ("SCA")

242. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

243. Under the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 et seq., "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

244. Section 2702(a)(2) of the SCA further states:

> [A] person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service (A) on behalf of, and received by means of electronic transmission from (or created by means of electronic transmission from), a subscriber or customer of such service; [or] (B) solely

> for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for the purposes of providing any services other than storage or computer processing….

245. The SCA creates a private right of action for those "aggrieved by any violation" of its provisions. 18 U.S.C. § 2707(a).

246. The conduct of T-Mobile, as alleged herein, constitutes a knowing and/or intentional violation of the SCA's Section 2702(a).

247. Plaintiff has been "aggrieved" by the conduct of T-Mobile, as alleged herein, in that Plaintiff's property has been stolen as described herein.

248. Pursuant to the applicable provisions of the SCA, Plaintiff is entitled to actual and statutory damages, as well as reasonable attorneys' fees and costs. 18 U.S.C. § 2702(c).

COUNT VIII
Violation(s) of the Computer Fraud and Abuse Act ("CFAA")

249. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

250. The CFAA governs those who intentionally access computers without authorization or who intentionally exceed authorized access and as a result of such conduct, cause damage and loss.

251. As set forth in the CFAA, the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter

information in the computer that the accesser [*sic*] is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

252. As alleged herein, a SIM-swap attack requires the intentional access to customer computer data by T-Mobile which exceeds its authority, and which conduct has caused damage and loss.

253. This access is often obtained through the use of T-Mobile credentials and T-Mobile property, such as REMO devices.

254. T-Mobile is subject to the provisions of the CFAA.

255. T-Mobile's conduct, as alleged herein, constitutes a knowing violation of the CFAA.

256. T-Mobile is also liable for the acts, omissions, and/or failures, as alleged herein, of any of its officers, employees, vendors, agents or any other person acting for or on behalf of T-Mobile.

257. T-Mobile violated its duty under the CFAA by exceeding its authority to access the computer data and breach the confidentiality of the proprietary information of Plaintiff by using, disclosing, or permitting access to Plaintiff's account, information, CPI and/or CPNI without the consent, notice and/or legal authorization of Plaintiff as required by the CFAA.

258. Section 1030(g) of the CFAA provides:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other

> equitable relief. A civil action for a violation of this section may be brought only if the conduct involved 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage….

259. Plaintiff alleged they have suffered damages which exceed the threshold of $5,000.00 as required by Section 1030(c)(4)(A)(i)(I) of the CFAA.

260. Plaintiff has brought this claim within two (2) years of the date of discovery of the damage pursuant to Section 1030(g) of the CFAA, or that time period has been tolled by the filing of arbitration by Plaintiff within those 2 years.

261. Upon information and belief, T-Mobile's conduct as alleged herein constitutes a violation of Section (a)(5)(A) of the CFAA.

262. Upon information and belief, T-Mobile's conduct as alleged herein may constitute an intentional violation of Section (a)(5)(C) of the CFAA.

263. As a direct consequence of T-Mobile's violations of the CFAA, Plaintiff has been damaged as set forth throughout this Complaint, plus fees and costs, including reasonable attorneys' fees.

COUNT IX
Conversion

264. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

265. On or around January 23, 2022 Plaintiff had actual or constructive possession of cryptocurrency, and/or an immediate right to possession of cryptocurrency as outlined throughout this Complaint.

266. T-Mobile USA, Inc., through their actions, inactions, conduct and policies (which continue through today) deprived Plaintiff of their right to that property.

267. T-Mobile USA, Inc., through their actions, inactions, conduct and policies (which continue through today) deprived Plaintiff of their use or possession of that property.

268. T-Mobile USA, Inc., through their actions, inactions, conduct and policies (which continue through today) have interfered with Plaintiff's property.

269. The aforementioned actions, inactions, conduct and policies deprived Plaintiff of their property and interfered with that property without Plaintiff's consent and without legal justification.

270. Plaintiff has suffered and will continue to suffer damages due to the conduct of T-Mobile USA, Inc., as set forth herein.

COUNT X
Civil Conspiracy

271. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

272. As set forth throughout this Complaint, there did exist a combination of two or more persons acting with a common purpose to do an unlawful act, namely to deprive Plaintiff of their right to, possession, and use of their cryptocurrency.

273. T-Mobile has taken multiple steps to effectuate that common purpose, through swapping Plaintiff's SIM-card, attempting to remove Plaintiff's ability to pursue damages and causes of action through edits to their Terms and Conditions, logging into Plaintiff's cryptocurrency account(s), stealing Plaintiff's cryptocurrency, concealing the identities of those individuals responsible, and refusing to provide information which would have allowed Plaintiff to attempt to regain their property.

274. T-Mobile took these actions without justification, and with the intent to injure Plaintiff.

275. As a result of those actions, inactions, conduct and policies of T-Mobile, Plaintiff has suffered, and will continue to suffer damages as set forth herein.

COUNT XI
Civil Aiding and Abetting

276. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

277. There does exist an independent wrong, including that Plaintiff had their cryptocurrency stolen.

278. T-Mobile USA, Inc., knew of the existence of those wrongs, including the theft of Plaintiff's cryptocurrency.

279. T-Mobile USA, Inc. provided substantial assistance in effectuating that wrong, including but not limited to: providing access to Plaintiff's accounts through T-Mobile credentials and property; concealing that access for a period of time; concealing, intentionally destroying and/or failing to preserve evidence necessary to track those individuals responsible for the theft; failing to report the associated criminal activity to law enforcement; and taking steps to conceal the identifies of those individuals responsible for the theft.

280. As a result of those actions, inactions, conduct and policies of T-Mobile, Plaintiff has suffered, and will continue to suffer damages as set forth herein.

COUNT XII

Breach of Implementing Regulations of FCA, 47 C.F.R. § 64.2001 *et seq.*

281. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

282. 47 CFR § 64.2010(b) provides: "The purpose of the rules in this subpart is to implement section 222 of the Communications Act…."

283. 47 CFR § 64.2010(a) provides:

> Safeguarding CPNI. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

284. In addition, subpart 64.2010(b), (d) and (e) further provide:

> Telephone access to CPNI. Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (c) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.
>
> ***
>
> In-store access to CPNI. A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.
>
> ***
>
> To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information.

285. Telecommunications carriers who rely on oral directions from customers "shall bear the burden of demonstrating that such approval has been given in compliance with the Commission's rules in this part." 47 CFR § 64.2007(1).

286. The information accessed by and/or disclosed to third parties by T-Mobile in the January 23, 2022 SIM-swap transferring control of Plaintiff's telephone number was CPI and CPNI under Section 222 of the FCA.

287. T-Mobile failed to protect the confidentiality of Plaintiff's account, CPI and CPNI, including their wireless telephone number, account information, and their private communications, by divulging or otherwise allowing access to that information to third parties on or around January 23, 2022.

288. Through its negligence, gross negligence, and deliberate acts – including inexcusable failures to follow its own security procedures, the CPNI Regulations, the warnings of the Pretexting Order, its Privacy Policy, COBC, Terms and Conditions, and CPNI Policy; and by allowing its employees, officers, vendors and/or agents to bypass such procedures, and failing to supervise/train its employees, officers, vendors, dealers and/or agents, T-Mobile permitted third parties to access Plaintiff's telephone number, telephone calls, text messages, cloud data, backups, emails, and account information to steal more than $290,429.12 worth of Plaintiff's property.

289. As a direct and proximate result of T-Mobile's violations, Plaintiff has been damaged by their loss of more than $290,429.12 worth of cryptocurrency which T-Mobile facilitated and allowed to be taken from them, and for other damages in an amount to be proved at any ultimate hearing or trial.

290. Plaintiff is also entitled to an award reimbursing them for attorneys' fees under the FCA in bringing this action against T-Mobile for T-Mobile's gross

negligence and fraudulent misrepresentations as to the security that it provides for customer accounts as required by the FCA and the CPNI Regulations.

COUNT XIII
Violation(s) of the California Constitutional Right to Privacy

291. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

292. The California Constitution declares that "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. Art. I, § 1.

293. Plaintiff has a reasonable expectation of privacy in their mobile device and their T-Mobile account information.

294. T-Mobile intentionally intruded on and into Plaintiff's solitude, seclusion, or private affairs by allowing its employees and third parties to improperly access Plaintiff's confidential T-Mobile account information without proper consent or authority.

295. The reasonableness of Plaintiff's expectations of privacy are supported by T-Mobile and its agents' unique position to safeguard their account data, including the sensitive and confidential information contained therein, and protect Plaintiff from SIM-swap attacks.

296. T-Mobile and its agents' intrusions into Plaintiff's privacy are highly offensive to a reasonable person. This is evidenced by federal legislation enacted by

Congress and rules promulgated and enforcement actions undertaken by the FCC aimed at protecting T-Mobile customers' sensitive account data from unauthorized use or access.

297. The offensiveness of T-Mobile's conduct is exacerbated by T-Mobile's material misrepresentations to Plaintiff concerning the safety and security of their account, while simultaneously making surreptitious edits deep into their impenetrable Terms and Conditions in a disgusting attempt to protect themselves while neutering their customer's ability to obtain redress for the negligence and other actions of T-Mobile.

298. Plaintiff suffered great personal and financial harm by the intrusion into his private data and accounts, as detailed throughout this document and as will be proven at any ultimate hearing and/or trial.

299. T-Mobile's actions and conduct complained of herein were a substantial and proximate factor in causing the harm suffered by Plaintiff. But for T-Mobile's agents', vendors' and employees' unauthorized access to Plaintiff's account, and T-Mobile's failure to protect Plaintiff from T-Mobile's own employees, agents and vendors through adequate security, training and oversight systems and procedures, Plaintiff would not have had their personal privacy violated and would not have been a victim of SIM-swap theft resulting in their loss of over $290,429.12 and the breach of sensitive personal information.

300. As a result of T-Mobile's actions, Plaintiff seeks actual and punitive damages in an amount to be determined at any ultimate hearing and/or trial in this matter. Plaintiff seeks punitive damages because T-Mobile's actions were malicious, oppressive, and willful. T-Mobile knew of the risks faced by Plaintiff, and the consequences of such risks. Nonetheless, T-Mobile failed to protect Plaintiff, and instead has apparently invested into a scheme to profit from SIM-swaps through an app known as "ZenKey." Punitive damages are thus warranted in order to deter T-Mobile from engaging in future misconduct.

COUNT XIV
Violation(s) of the California Consumer Privacy Act

301. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

302. The California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 et seq.) ("CPA") provides that "[a] business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure…." Cal. Civ. Code § 1798.100(e).

303. Respondent T-Mobile is a covered entity under the California Consumer Privacy Act as a business that collects consumer personal information.

304. As detailed throughout this document and as will be proven at any ultimate hearing or trial in this matter, T-Mobile has failed to implement reasonable

security procedures and practices to protect the personal information of its customers from unauthorized or illegal access, destruction, use, modification or disclosure.

305. The CPA further states that "[a]ny consumer whose nonencrypted and nonredacted personal information…or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for…actual damages…injunctive or declaratory relief [and] any other relief the court deems proper."

306. As detailed throughout this document and as will be proven at any ultimate hearing or trial in this matter, Plaintiff's personal information was stolen as a result of T-Mobile's violation of their duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's personal information and has suffered damages in excess of $290,429.12 as a result.

COUNT XV
Breach of Contract

307. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

308. Plaintiff was a customer of Defendant T-Mobile and had a contract for service with Defendant T-Mobile.

309. A vital component to Defendant's performance of that contract was T-Mobile's responsibility to safeguard Plaintiff's information, including sensitive personal and financial data.

310. T-Mobile's responsibilities to safeguard Plaintiff's sensitive personal information are outlined, among other places, in T-Mobile's own policies, and include promises not to sell or disclose users' personal information to any unauthorized parties, T-Mobile's use of safeguards to protect that information, and T-Mobile's commitment to, and implementation of, policies and procedures to ensure compliance with state and federal laws involving data brokers and common carriers.

311. As stated by T-Mobile on their Data Transparency / CPNI Website: "[u]nder federal law, you have a right, and we have a duty, to protect the confidentiality of CPNI."

312. T-Mobile breached their obligations and duties by failing to implement systems and safeguards that would protect Plaintiffs' personal information and limit access of this information to authorized scenarios and individuals.

313. T-Mobile also breached these duties of care when their agents allowed access and changes to Plaintiff's account by turning over control of Plaintiff's phone number to either themselves or an unidentified individual.

314. T-Mobile's actions in handing over full access to Plaintiff's entire digital presence, including unrestricted access to Plaintiff's cloud data, backups, information, account and finances, is a grave breach of their duties.

315. Were it not for T-Mobile's actions, Plaintiff would not have suffered any damages.

316. As a result of the foregoing acts by T-Mobile, Plaintiff has been damaged in an amount to be determined at trial.

COUNT XVI
Breach of Fiduciary Duty

317. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

318. Plaintiff gave their personal information and entrusted T-Mobile with sensitive information in order to use that service, and as a result, T-Mobile owed a duty of care in how it utilized and protected that information.

319. This placed T-Mobile in a position of being a fiduciary to Plaintiff and the sensitive personal and financial data Plaintiff entrusted T-Mobile with.

320. T-Mobile's breach of security in handing over full access to Plaintiff's sensitive personal information and financial access is not just a breach of federal and state laws, but a breach of this duty of care.

321. As a result of the foregoing acts by T-Mobile, Plaintiff has been damaged in an amount to be determined at trial

COUNT XVII
Violations of the Fair Credit Reporting Act

322. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

323. The Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*. contains the Red Flags Rule (16 CFR Part 681).

324. That Rule requires many businesses and organizations to implement a written identity theft prevention program designed to detect the "red flags" of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate its damage.

325. The rules are intended to help businesses spot suspicious patterns and prevent the costly consequences of identity theft.

326. T-Mobile is a covered entity under the Red Flags Rule and the Fair Credit Reporting Act.

327. The SIM-swap at issue in this matter and the CPNI breach associated with the same is covered under the Red Flag Rule's definition of "identity theft" which provides the term "identity theft" means "a fraud committed or attempted using the identifying information of another person without authorized." Federal Register Vol. 72, No. 217, Friday, November 9, 2007 Rules and Regulations, pg. 63723.

328. "Identifying information" is defined as including "[t]elecommunication identifying information." Id.

329. Upon information and belief, T-Mobile's actions as described throughout this document and as will be established after discovery constitute multiple violations of their duties under this statute, including failing to: have an adequate program in place to identify, mitigate and prevent identity theft as suffered by Plaintiff; train staff

as necessary; monitor the activities of their service providers; and secure the data they collect and maintain about their customers.

330. As a result of the foregoing acts by T-Mobile, Plaintiff has been damaged in an amount to be determined at trial.

COUNT XVIII
Declaratory Judgment

331. Plaintiff incorporates by reference all facts and allegations of this document, as if the same were fully set forth herein.

332. Plaintiff brings this claim for declaratory relief under 28 U.S.C. § 2201 to request a declaration that T-Mobile's wireless customer agreement set forth in the T-Mobile T&Cs (the "Agreement) is unconscionable, void against public policy, and unenforceable in its entirety.

333. Plaintiff disputes that the Agreement was ever presented to him prior to initiating service or bringing his claims. But to the extent that the Agreement was purportedly presented, it would have been presented to Plaintiff, like all other wireless users, on a take-it-or-leave-it basis.

334. The Agreement was thereafter changed an unknown number of times, without being presented to Plaintiff or notifying Plaintiff of material changes. Plaintiff had no ability to negotiate any term of the agreement. In contrast, T-Mobile has virtually unlimited power over its customers, including Plaintiff, as seen herein by virtue of the fact that T-Mobile purports to hold Plaintiff and all other wireless users to the burdensome terms of an agreement that they may well have never seen, read,

negotiated, asked questions regarding, or understood. This is particularly salient where Plaintiff's service was initiated with T-Mobile by someone else on Plaintiff's behalf, or where Plaintiff's first language was not English.

335. The version of the Agreement in effect when Plaintiff suffered the SIM-swap detailed herein purports to govern T-Mobile's provision of wireless service to all customers, including Plaintiff.

336. The Agreement contains numerous unconscionable terms that render it unenforceable in its entirety because its central purpose is tainted with illegality.

337. The Agreement states that it includes not only T-Mobile's T&Cs, but also "the additional terms found in your Rate Plan, your Data Plan, your Service Agreement, and provisions linked to from these T&C." The agreement further obliquely references the applicability and incorporation of a potentially unlimited number of statutes and other policies of T-Mobile so that it is impossible to effectively discern what the Agreement reads as a whole.

338. Additionally, the Agreement states that T-Mobile "may change, limit, suspend, or terminate your Service or this Agreement at any time…." Through such language, T-Mobile apparently contends that not only the Agreement, but all other agreements and terms referenced therein, bind all wireless customers, whether or not such customers have seen the Agreement, can understand the Agreement, can read the Agreement, or are even aware of its existence. In other words, every time (and at any time) T-Mobile creates a new and more onerous version of its documentation, their

unsuspecting customers are purportedly bound by the new terms. This practice highlights the fact that not only are these contracts not negotiable, but they are also invisible. What you don't see, you still get.

339. The Agreement is a classic contract of adhesion imposed by T-Mobile upon a party with no bargaining power. In contrast, T-Mobile has unchecked power to insist upon its own terms even if the consumer is unaware of or disagrees with the terms of the Agreement itself. There is no ability to negotiate any term of the Agreement. It is literally "take it or leave it."

340. The Agreement is void as against public policy as a contract of adhesion purporting to bind customers who have never heard of or seen the Agreement, and are most likely entirely unaware of its provisions and their meanings, including deceptively placed and dissected provisions placed deep into an unpaginated document.

341. The Agreement is void and unenforceable in its entirety because it also purports to contain exculpatory provisions, damage waivers, references to an unknowable amount of other documents, laws, policies and statutes, and an indemnification provision that purports to prevent consumers from bringing any claims against T-Mobile.

342. The exculpatory provision in the Agreement ("Exculpatory Provision") contains numerous provisions that are contrary to public policy because they attempt

to exempt T-Mobile from responsibility for its own gross negligence, fraud, and violations of law.

343. The Exculpatory Provision renders the entire Agreement unenforceable on public policy grounds because it purports to exempt T-Mobile from its own gross negligence, statutory violations, and willful behavior.

344. Moreover, the Exculpatory Provision is contained in a complex, lengthy and unpaginated contract that provides essential wireless services – without which most customers have no means of communication (including for emergency services), let alone essential computing, geolocation, texting, research or other services.

345. The Exculpatory Provision – included in a contract of adhesion as to which T-Mobile's users, including Plaintiff, have no bargaining authority—is void because it is plainly unconscionable and against public policy.

346. The Exculpatory Provision is also substantively unconscionable because it allocates risks in an objectively unreasonable manner.

347. The allocation of risks under the Agreement are objectively unreasonable because T-Mobile – a telecommunications behemoth with billions of dollars of assets and tens of millions of customers – takes upon itself virtually no liability and purports to exempt itself from virtually all damages.

348. The Agreement is further unenforceable because customers are purportedly required to indemnify T-Mobile for all claims arising out of the services

provided by T-Mobile, including claims that arise due to T-Mobile's negligence, gross negligence, deliberate conduct, or statutory violations.

349. The indemnity provision in the Agreement ("Indemnification") states:

> You agree to defend, indemnify, and hold us and our directors, officers, and employees harmless from any claims arising out of use of the Service or Devices, breach of the Agreement, or violation of any laws or regulations or the rights of any third party by you, any person on your account or that you allow to use the Services or your Device.

350. Read literally, the Indemnification arguably requires a consumer, such as Plaintiff, to hold T-Mobile harmless for T-Mobile's own negligence, deliberate behavior, gross negligence, statutory violations (including disclosure of CPNI under the FCA), or fraud for any conduct arising out of "use of the Service" or even T-Mobile's "breach of the Agreement."

351. On its face, the indemnity provision in a contract of adhesion renders the entire Agreement unconscionable and unenforceable because it defeats the entire purpose of the contract by making it impossible for consumers to bring claims against T-Mobile for the entire range of statutory rights to which a consumer, such as Plaintiff, is entitled.

352. Indeed, the Indemnification would arguably totally obviate T-Mobile's commitment to privacy in its Privacy Policy as well as its legal obligations under statutes such as the FCA and the CPNI Rules.

353. Because the entire Agreement is unenforceable due to the central purpose of the Agreement being tainted with illegality so that the contract as a whole cannot be enforced, the arbitration provision in the Agreement ("Arbitration Provision") is also unenforceable.

354. T-Mobile's reading of the Arbitration Provision would arguably require Plaintiff to arbitrate their claims without affording the full range of statutory remedies, including indirect, special, consequential, treble or punitive damages that are available to them under the claims alleged herein.

355. Moreover, T-Mobile's reading of the Arbitration Provision may require Plaintiff to forego the full range of damages to which they are entitled under their claim for relief under the Federal Communications Act § 222.

356. These defects render not only the Arbitration Provision, but also the entire Agreement unenforceable.

357. The Agreement and enforcement of its terms is further unconscionable because Plaintiff was never presented with the ability to read, negotiate and understand prior to those terms being applied against him, and T-Mobile failed to notify Plaintiff of material changes to the Agreement throughout the life of his account, yet seeks to bind him to the same.

358. The FAA provides that an arbitration agreement may be declared unenforceable "upon such grounds as exist at law or in equity for the revocation of

any contract," including "generally applicable contract defenses, such as fraud, duress, or unconscionability." 9 U.S.C. § 2.

359. There is an actionable and justiciable controversy between Plaintiff and T-Mobile in that Plaintiff contends that the Agreement, including the Exculpatory Provision, Indemnification, and Arbitration Provision, is unenforceable in its entirety because it is unconscionable and void against public policy since it arguably prevents consumers, such as Plaintiff, from obtaining redress from T-Mobile even for deliberate acts in violation of its legal duties.

360. A declaration of the enforceability of the Agreement is thus necessary and appropriate.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests judgment in their favor and against Defendants, and for the following:

A. Judgment for Plaintiff on all counts.

B. Actual damages.

C. Incidental damages.

D. Consequential damages.

E. Statutory damages.

F. Treble damages.

G. Punitive damages.

H. Attorneys' fees.

I. Costs and expenses.

J. Injunctive relief.

K. Declaratory relief.

L. Sanctions.

M. Pre- and post-judgment interest; and

N. Such other relief as deemed just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a trial by jury of all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

DATED: January 16, 2024

Respectfully submitted,

/s/ Kent Petry

Kent Petry
LAW OFFICES OF KENT PETRY
1135 Mearns Road, #3387
Warminster, PA 18974
Telephone: 215-322-1084
Facsimile: 215-798-8054
Email: kent@petrylaw.net
Admitted Pro Hac Vice

Amy K. Saechao (Bar No. 336693)
NEXT LEVEL LEGAL
6080 Center Drive, Suite 600
Los Angeles, CA 90045
Telephone: 310-426-8823
Email: amy@nextlevellegal.com
Counsel for Jesus Marcos